

---

# **Enterprise Dynamic Access Control (EDAC) Overview**

**Prepared for  
Commander, U.S. Pacific Fleet  
Pearl Harbor, HI 96860**



**Prepared by  
Richard Fernandez  
SSC San Diego  
675 Lehua Ave, Building 992  
Pearl City, HI 96782  
(808) 474-9270, fax (808) 471-5837  
[richard.r.fernandez@navy.mil](mailto:richard.r.fernandez@navy.mil)**

## Revisions

Publication Debut

May 1, 2005

Richard Fernandez

## Acknowledgements

The author also wishes to acknowledge the following COMPACFLT Secured Enterprise Access Tool (SEAT) architects: Wallace Fukumae, Tuan Huynh , Wilfredo Alvarez, Ryan Kanno, Dean Tanabe.

## Trademarks

Company names are registered trademarks or trademarks of their respective companies.

## Invention Disclosure

The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189.

## Resources

National Institute of Standards and Technology, Role Based Access Control:  
<http://csrc.nist.gov/rbac/>

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

## CONTENTS

Contents.....	ii
Abstract.....	1
Enterprise Dynamic Access Control (EDAC) .....	2
Limitation of access control list (ACL) and groups.....	2
Objects .....	2
Environmentals .....	2
Complexes.....	2
Enterprise and remote configuration requirements.....	3
Modular access control model .....	3
EDAC Component overview .....	3
References.....	5
References represent objects.....	5
References represent environmentals .....	5
References represent complexes .....	6
Reference structures.....	7
Reference used as conditions.....	8
Reference used as inputs.....	8
Customer Meta-Database (CMD) .....	10
Resource Profiles.....	11
Structure Format Service (SFS).....	14
Condition Deprecator Service (CDS) .....	16
Enterprise Interoperability .....	16
Summary.....	18

## ***Abstract***

The Enterprise Dynamic Access Control (EDAC) represents an access control model that adheres to the basic principles of Role-Based Access Control (RBAC) standard published by the National Institute of Standards and Technology (NIST). The EDAC accommodates complex and scalable access control situations many government and civilian organizations are experiencing when managing resource access.

Access control is the process that evaluates resource access. Resources can represent software applications, web services and even facility access. An effective access control model should be capable of evaluating resource access based on user characteristics and environmental factors. Currently, access control lists (ACL) and groups represent static listings of individual names allowed access to resources. This per person approach of establishing resource access becomes unmanageable as the number of users requiring resources access grows. Unlike static listings, the EDAC criteria for resource access are based on user characteristics and environmental factors. This access control system establishes an effective security policy and accommodates enterprise implementations among regions. Static listings offer little in the way of hierarchical considerations or inheritance of permissions but the EDAC can evaluate inheritance on every user characteristic and environmental factor. Static listings are incapable of altering resource access based on changes due to security advisories (such as Homeland Security) but the EDAC can accommodate such changes with pre-configured conditions.

## ***Enterprise Dynamic Access Control (EDAC)***

### **Limitation of access control list (ACL) and groups**

Determining access to resources such as software applications and web services are becoming increasingly difficult to manage via access control lists (ACLs) or group based policies. These static listings usually determine resource access by evaluating an object's name or unique identifier. Groups determine resource access by evaluating a single object characteristic. However, resource access is usually based on the evaluation of multiple object characteristics contained in an **object profile**.

### **Objects**

An **object** is a person or thing seeking resource access. An object profile contains a compilation of user characteristics such as: corporate assignment, security clearance, job description and/or salary. If there is a corporate reassignment or security clearance change access to resources may be affected. Unfortunately static listings cannot accommodate such critical changes unless resource managers (RM) constantly monitor personnel records and implement immediate changes. Such a task can become unmanageable as the number of users and resources grow. Limitations to personnel records by RM enterprise-wide could compound the problem. In the Enterprise Dynamic Access Control (EDAC) model, a RM is not required to query personnel records. Instead, a RM simply establishes conditions based on a user's characteristics.

### **Environmentals**

Another important access control requirement is the establishment of **environmental** conditions. Environmentals are non-object related events that can change over time such as: security advisories and time. Homeland Security and regional Information Assurance agencies are authorized to impose security warnings that may affect access to a wide range of resources by many personnel. Sudden changes in security conditions may not allow sufficient time to update static listings, thereby creating a possible security breach by unauthorized personnel. Finer granularity of resource access may be required during certain security levels. For example, during Homeland Security Advisories: *Severe* and *High*, only *administrator* and *superuser* account holders would be granted access to a particular resource, while all *guest* and *user* account would be denied access. An EDAC solution can accommodate these kinds of scenarios by pre-configured conditions for each respective security level. For example, if a Homeland Security Advisory changes, the EDAC only evaluates the conditions established for the prevailing security level. The EDAC can also accommodate corporate customized security advisories.

### **Complexes**

A third criterion to determine resource access is a function of object and/or environmental values. The capability to process certain object characteristics and/or environmental status through an operation that produces an output is then evaluated to determine resource access. This type of condition is referred as a **complex**.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

### **Enterprise and remote configuration requirements**

Because RMs are located at various locations a **condition manager service (CMS)** serves as an interface to corporate directory services. These corporate directory services contain object, environmental and complex conditions and are referred as a **customer meta-database (CMD)**. Centrally managed CMD(s) offer RMs a reliable and synchronized data store of conditions. This architecture also allows RM the capability to establish conditions for remote users furnishing an enterprise-side access control solution. Because content in directory services is structured selection of conditions from such a platform allows hierarchy or inheritance evaluation.

### **Modular access control model**

Existing industry access control products currently require a proprietary commitment. A concern with access control proprietary solutions is the lack of standard tie-ins with customer assets. A standardless access control tie-in with customer assets leaves the customer at a disadvantage because proprietary solutions require some level of customization and maintenance. Customization also leaves the customer at risk if the servicing access control product can no longer be vendor supported. These unforeseen changes can quickly leave a customer's access control solution vulnerable. The consequences could be wide-ranging and significant since access control is tightly coupled with security. The only other alternative for the customer is to abandon the current access control infrastructure and replace it with another proprietary solution. This "fork-lift" approach leaves a customer with financial burdens and disruption of services. For this reason, some customer's have developed an in-house access control solution because it assures continued supportability but this option presents a significant cost.

### **EDAC Component overview**

The EDAC is a modular access control environment with defined customer integration. If integration becomes standardized interchangeable access control solutions could seamlessly interface with customer assets. This approach would void the costs of custom coding interfaces and offer long-term support.

Figure 1 illustrates an overview and summary of the EDAC model.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

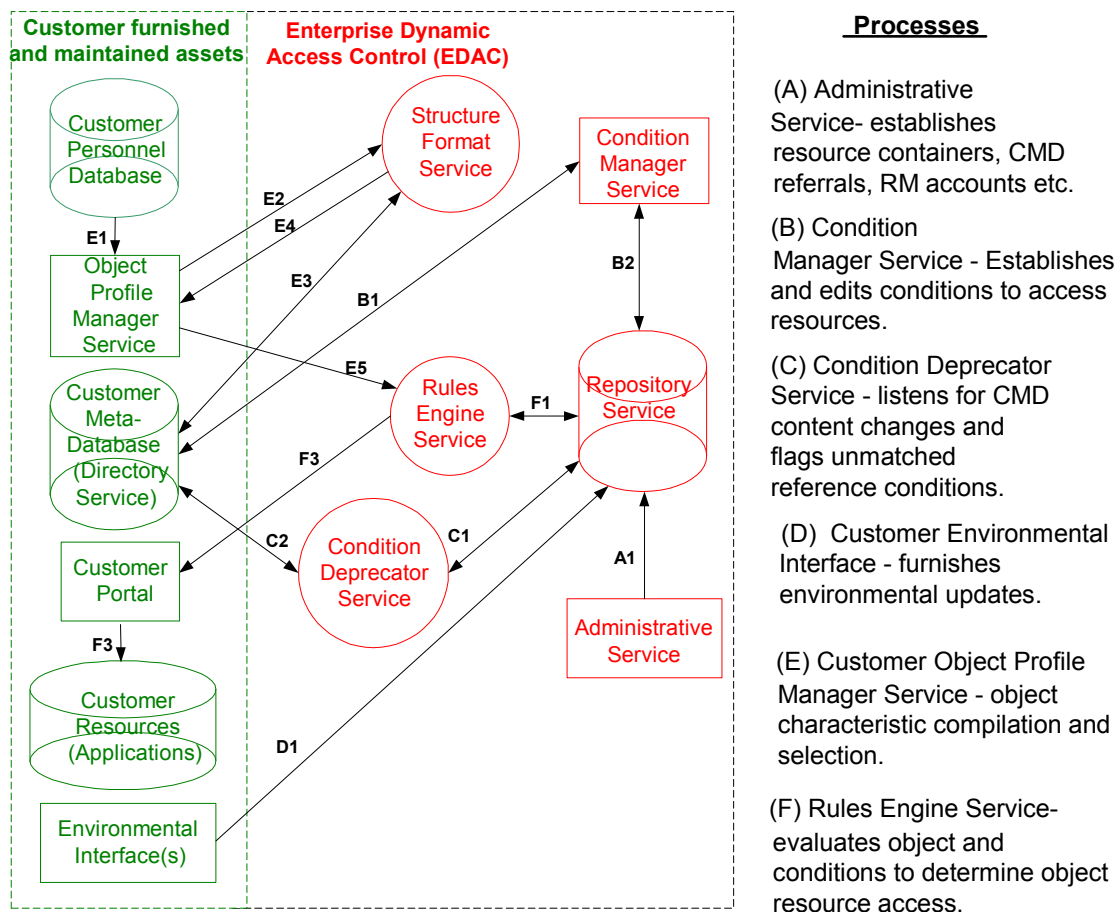


Figure 1

*Customer Personnel Database (CPD)* contains corporate and personnel data such as employee: salary, job description, organization assignment etc.

*Customer Object Profile Manager service (OPMS)* queries the *customer personnel database* and presents a compilation of user characteristics referred as a user profile.

*Customer Meta-Database (CMD)* contains data used to establish conditions for resource access. The data content consists of structured corporate characteristics such as: salary, job descriptions, organization structures and environmentals and complex data.

*Customer portal* interfaces with the EDAC to list accessible resources.

*Customer resources* represents software applications, web services, cipher locks, etc.

*Customer environmental interfaces* serves as an input for prevailing environmental statuses such as prevailing security levels (INFOCON, Homeland Security Advisory Levels, etc.), time, weather readings etc.

*Condition Manager Service (CMS)* is a web interface for RM to establish conditional access to *customer resources*.

*Rules Engine Service (RES)* evaluates object and conditions to determine resource access. Compares inputs such as object profiles and environmental statuses with pre-configured conditions.

*Repository Service (RS)* stores: resource access conditions, RM accounts and CMD connection parameters.

*Administrative Service (AS)* performs configuration management on content of *repository service*.

*Structure Format Service (SFS)* converts object profile and environmental status inputs to DN format by searching CMD.

*Condition Deprecator Service (CDS)* evaluates resource profile conditions with the current state of *customer meta-databases*. Deprecated conditions are flagged in the *condition manager service*.

## References

References are used to describe data and conditions about objects, environmentals and complexes. References consist of reference categories (RC) and corresponding reference values (rV).

### References represent objects

Object references consist of "object reference categories" or "**RCobj**" and are used to categorize data about an object, such as: "clearance", "paygrade", "job function", "employer", or "organization". An "object reference value" "**rVobj**" is used to describe the value under a specific RCobj.

Figure 2 illustrates an object reference:

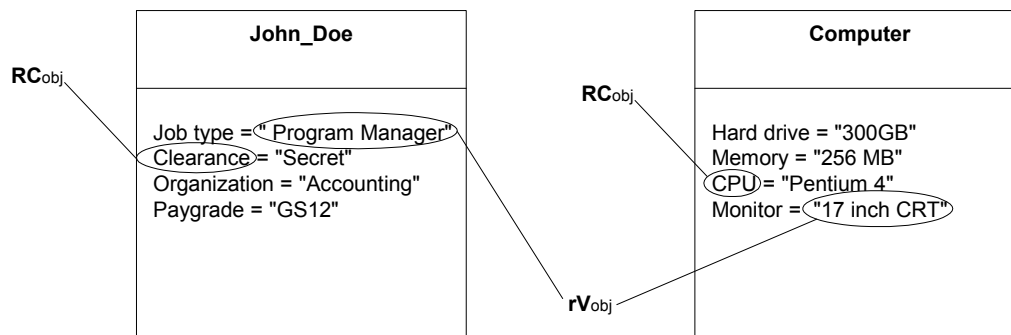


Figure 2

### References represent environmentals

Environmental references consist of "environmental reference category" or "**RCenv**" and are used to categorize data about an environmental, such as: "Time", "security level", or "temperature". An "environmental reference value" "**rVenv**" is used to describe the value under a specific RCenv.

Figure 3 illustrates an environmental reference:



"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

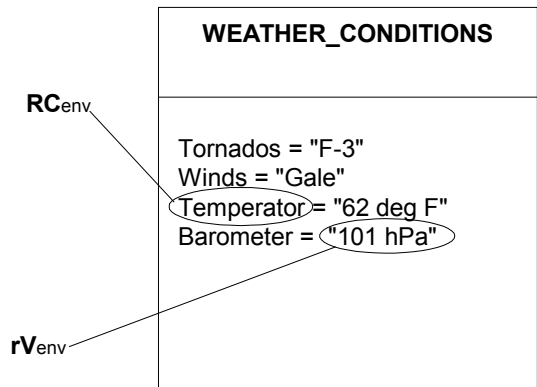


Figure 3

**References represent complexes**

Complex references consist of “complex reference categories” or “**RCcpx**” and are used to categorize output variables from a customized operation. Figure 4 illustrates a risk assessment **RCcpx** containing various **rVcpx** ranging from 1 – 10.

**COMPLEX output with a variable output.** **COMPLEX** variable outputs do have reference categories and reference values. A resource profile that contains a **COMPLEX** points to the **COMPLEX** operation. The operation will return reference category and corresponding reference value(s).

A table with 6 columns and 4 rows. The first column is labeled **Security Clearance**. The other five columns are labeled **Low**, **Guarded**, **Elevated**, **High**, and **Severe**. The rows are labeled **Top Secret**, **Secret**, and **Confidential**. The values in the table are as follows:

Security Clearance	Low	Guarded	Elevated	High	Severe
Top Secret	1	2	3	4	5
Secret	5	6	7	8	9
Confidential	6	7	8	9	10

Arrows point from the labels **RCobj**, **rVobj**, **RCenv**, and **rVcpx** to the corresponding parts of the table. **RCobj** points to the first column. **rVobj** points to the first three rows. **RCenv** points to the header row. **rVcpx** points to the values in the table.

Here is the **COMPLEX** operation that produces a variable output.



Figure 4

A complex operation could produce a Boolean outcome instead of a variable.

## Reference structures

A customer will use different reference structures to describe objects, environments and complexes within a CMD. In figure 5, RObj called "Job Descriptions" contains a list of rVobj, such as, Developer, Program Manager, and Chef, etc.

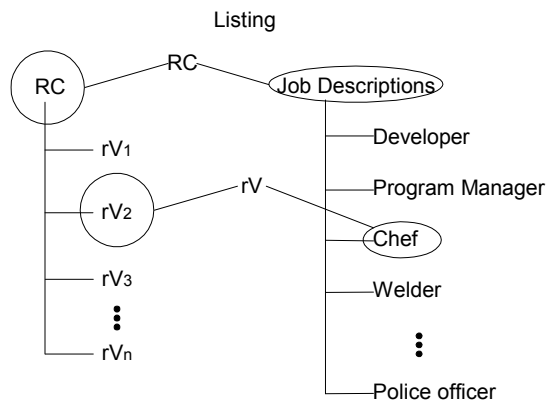


Figure 5

In figure 6, RObj called "ACME Corporation" contains a hierarchy of rVobj such as: Assembly Line, Parts, and Maintenance, etc.

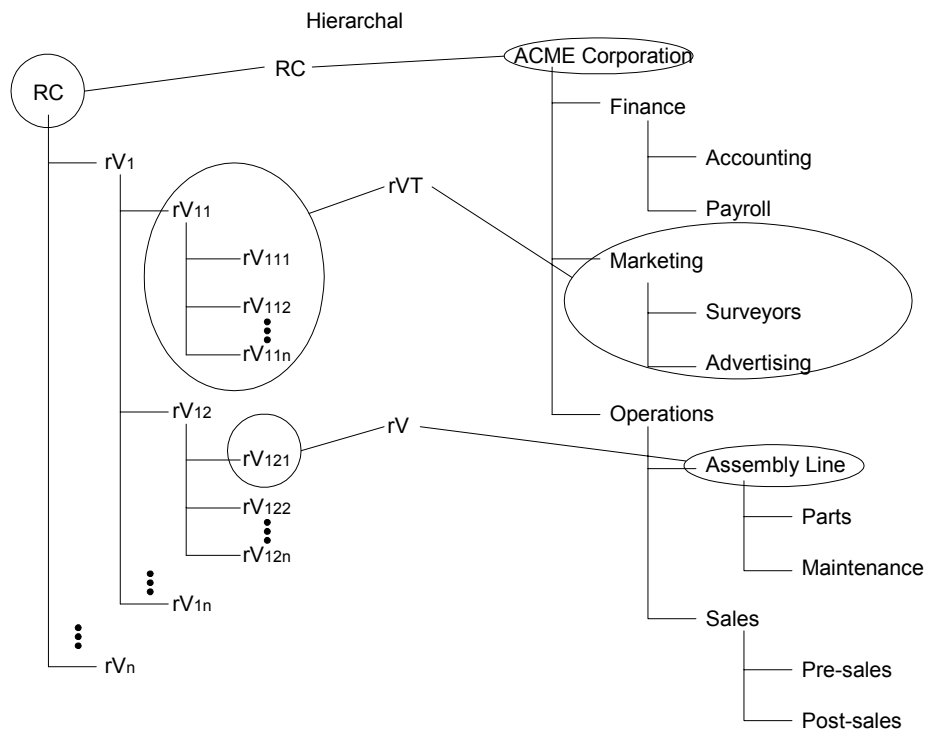


Figure 6

The abbreviation "rV" means a single reference value while "rVT" means a parent and all associated children "rV". Note in figure 5, "Marketing" represents an "rVT" with "rV" children: "Surveyors" and "Advertising". Therefore, a "rVT" includes one or more "rV". The selection of an rVT alleviates the RM from having to find and choose all sub tree conditions.

**Reference used as conditions**

References conditions are established by a RM(s) and evaluated by the EDAC rules **engine service (RES)** to determine resource access. **Reference conditions** can consist of object, environmental and complex references. Reference conditions can contain an unlimited number of: RCobj, RCenv, RCcpx and each RC can contain an unlimited number of rV and rVT. For example, in figure 6, above, a RM can select the following rV and rVT for the ACME Corporation RCobj as reference conditions:

rV = Assembly Line  
rVT = Marketing which contains rV = Marketing, Surveyors, Advertising.

These reference conditions as well as reference inputs would be evaluated by a RES to determine resource access.

**Reference used as inputs**

Reference inputs can only consist of object and environmentals. Reference inputs can contain an unlimited number of: RCobj, RCenv and each RC can contain only one rV. A compilation of rVobj is an **object profile** and represents a user's characteristics, as shown in figure 7:

Object Profile	
RCobj	rVobj
Paygrade	Wage Grade 12
Clearance	secret
Organization	Assembly Line
Job Title	Welder

Figure 7

A user can have multiple object profiles. **Customer personnel database(s) (CPD)** are queried to compile an object profile. Object profiles are compiled on a real time basis whenever an object seeks resource access by an **object profile manager service (OPMS)**.

Environmental references used as reference inputs are called **environmental status**. These environmental statuses are evaluated against any environmental reference condition, established by the RM.

Figure 8 illustrates how reference inputs and conditions interact in an EDAC model:

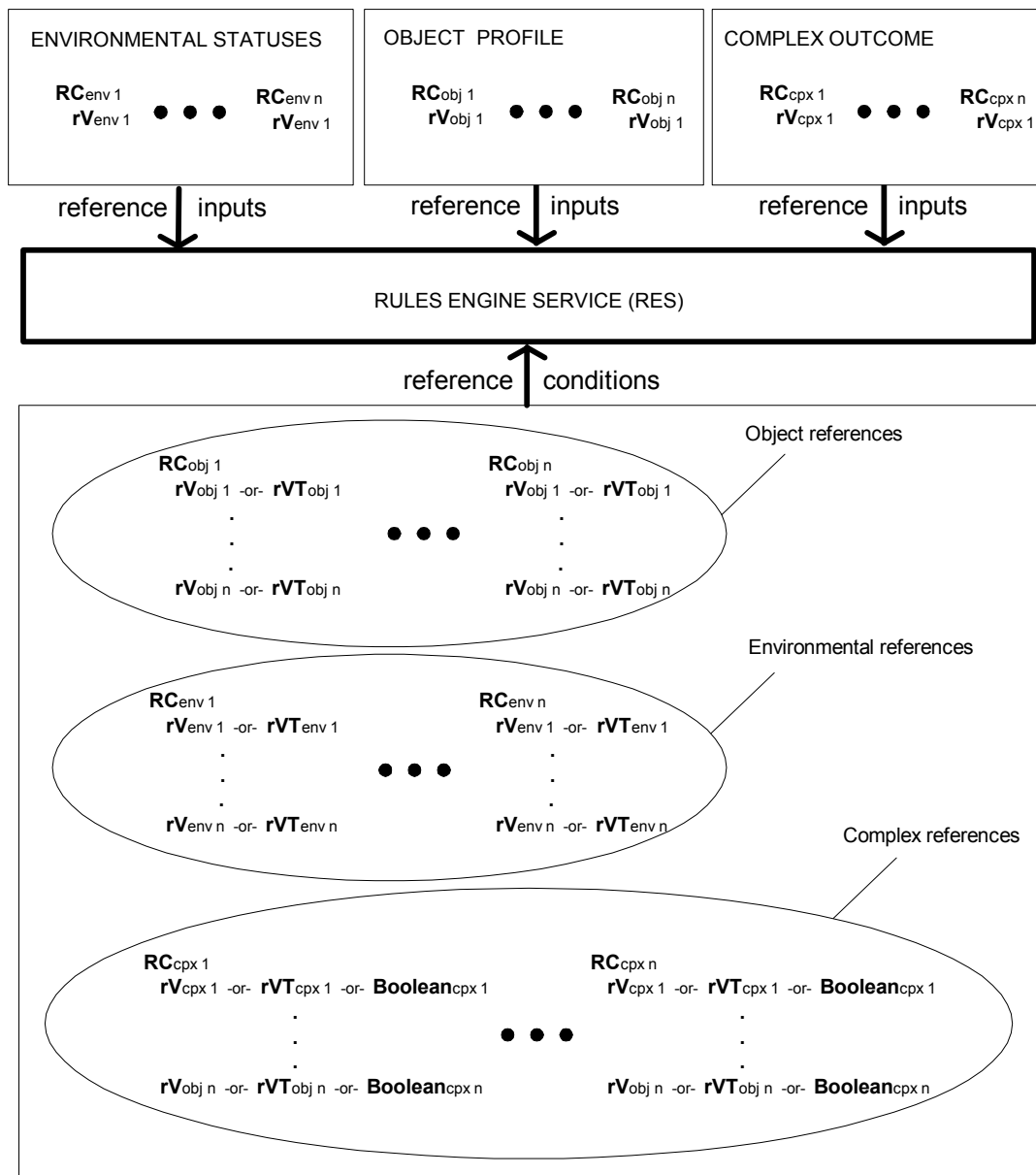


Figure 8

## Customer Meta-Database (CMD)

CMDs offer RMs the capability to remotely select reference conditions from synchronized, centrally managed and reliable data stores. Most organizations store information about employees and corporation in relational database(s). These databases are referred as **customer personnel databases (CPD)**. This data can be transposed to a structured format and placed in a directory service referred as a CMD. The CMDs are own, maintained and operated by the customer. Refer to figure 9.

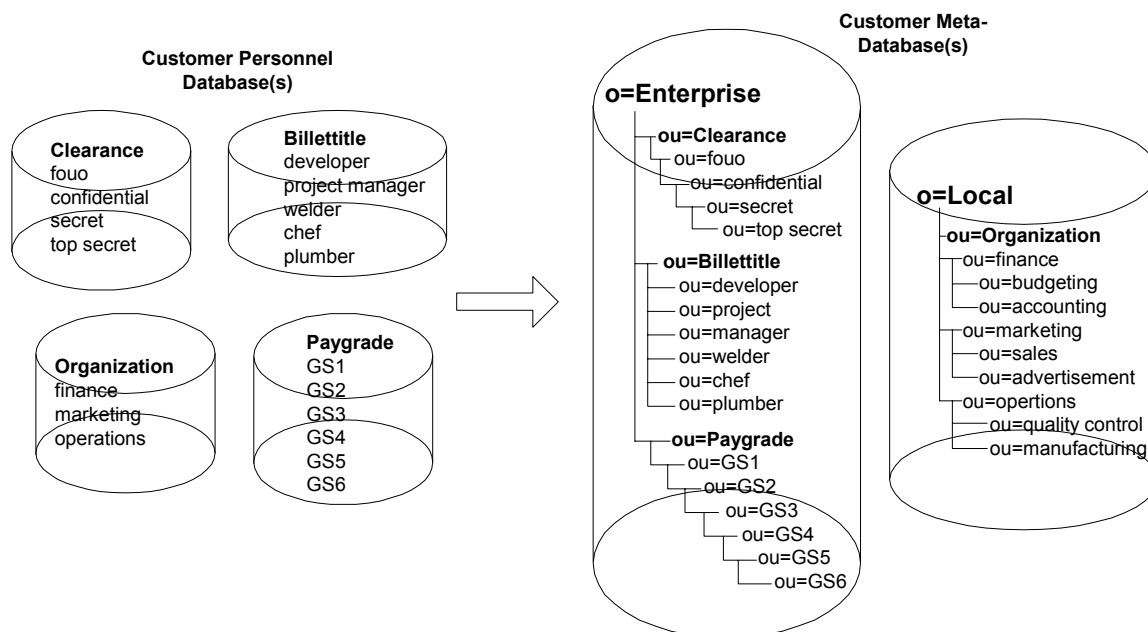


Figure 9

References can be distributed among many CMDs and managed by various organizations within a corporation or command. References can be maintained locally or globally within a community of interest. Figure 10 shows how a corporation could manage their own CMD domain. The corporation can consist of regional offices at different locations while the corporate headquarters can manage the global CMD(s).

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

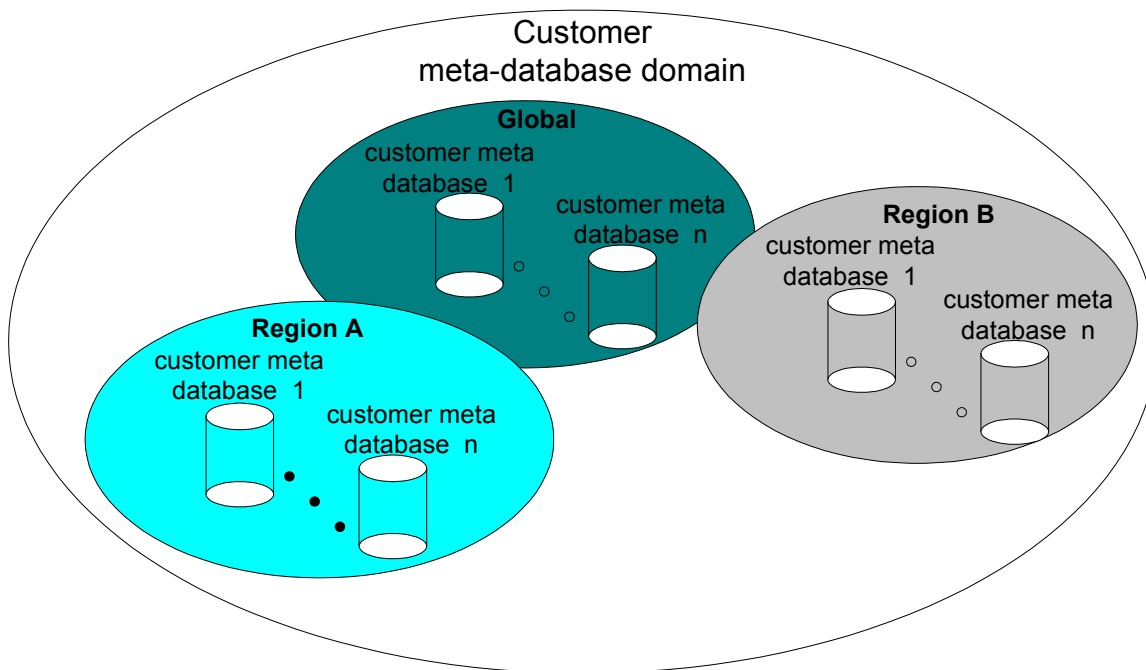


Figure 10

## Resource Profiles

A **resource profile** is a container consisting of a set of reference conditions that when evaluated with a reference input (such as object profile and/or environmental status) will determine if an object is allowed or denied access to a resource role. A match occurs when all reference conditions within a resource profile match an object profile and environmental status. There are two types of resource profiles: allow or deny. Reference conditions stored in resource profiles are in a structured format because such they are selected directly from a CMD. In figure 11, the CMD consist of a directory service whose selected references are in distinguished name format.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

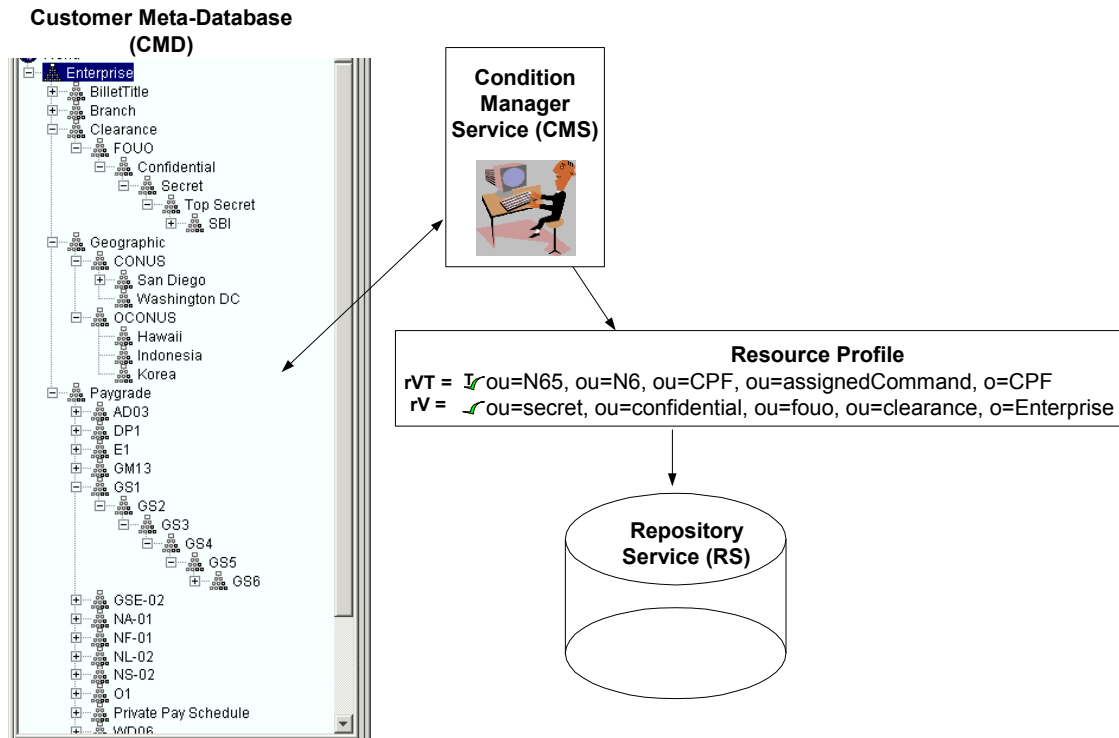


Figure 11

Resource access is granted if an object profile and/or environmental status match all reference conditions in an allow resource profile (ARP). A deny resource profiles (DRP) is optional and represents a filter for an ARP. This feature alleviates a RM from selectively establishing ARPs within a wide scope that excludes certain portions. For example, in figure 12 a RM allows resource access to all personnel who belong to the ACME Corporation but excludes the entire Finance and selected portion of the Sales departments.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

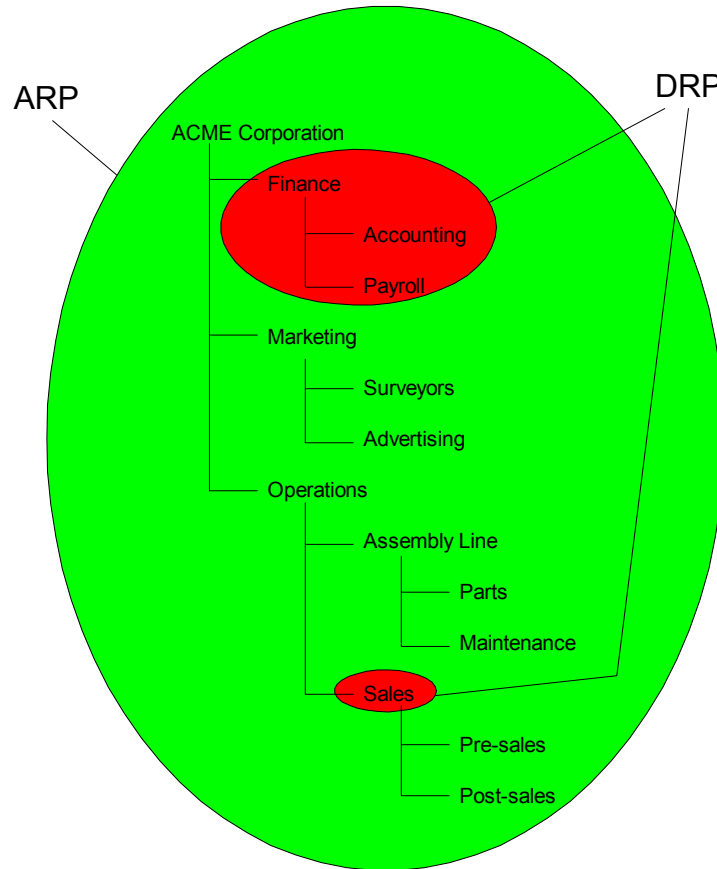


Figure 12

A RM can establish as many resource profiles as required to allow or deny access to a resource role. Deny resource profiles are evaluated first by the RES. An **access control role (ACR)** is a container consisting of a set of resource profiles. If any resource profile produces a match access can be granted or denied depending on type of resource profile. Figure 13 illustrates this point:



"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."



Resource	Enterprise Dynamic Access Control			
Resource Roles	Access Control Roles (ACR)	Resource Profiles		
Guest	Guest	CPF Guest T ✓ COMPACFLT	CSP Guest T ✓ COMSUBPAC	CNR Guests T ✓ COMNAVREG   Tuesdays 1700 -2300
User	User	CPF N6 Users T ✓ CPF N6 T ✓ GS12	Deny Contr Users T ✓ CPF N6 T ✓ Secret T ✓ CONTR	
Administrator	Administrator	CPF Admin T ✓ CPF N65 T ✓ TS	Deny CPF N65 Admin T ✓ CPF N65 T ✓ CONTR   Mon & Thurs 0800 -1300	

Figure 13

For example, if an object worked at CPF N6 and was a GS12 the *CPF N6 Users* allow resource profile (represented with a green checkmark) would produce a match and the object would be granted access under the *user* resource role. In another example, if an object worked at CPF N651, as a contractor the *Deny CPF N65 Admin* deny resource profile (represented with red checkmarks) would produce a match only during the hours of 0800-1300 and the object would be denied access to the *user* resource role. Note a “T” next to the checkmark represents a sub tree or “rVT” reference condition.

### Structure Format Service (SFS)

The SFS converts reference inputs such as an object profile, environmental status and/or complex outputs into a structured format that can be compared with reference conditions

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

stored in resource profiles. A CMD consisting of directory services requires the SFS to convert reference inputs into distinguished name format for evaluation by the RES. Refer to figure 14:

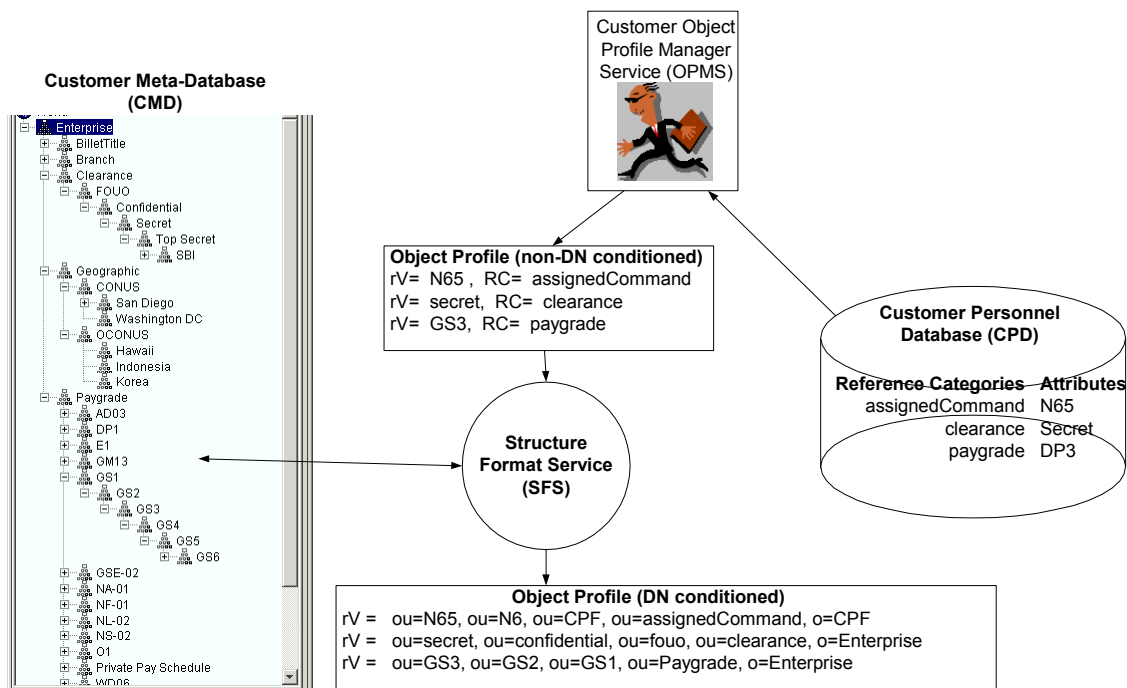


Figure 14

Since reference inputs are not in DN format the SFS queries domain CMDs and converts them into DN values. A DN reference represents a format that can be evaluated for inheritance purpose. For example, say a reference condition contained the following DN value:

rV: ou=secret, ou=confidential, ou=clearance

If an object profile contained the following reference input a match would not occur:

rV: ou=top secret, ou=secret, ou=confidential, ou=clearance

However, if the reference condition changed to a sub Tree a match would occur because it would represent all values equal or above *secret*, which includes *top secret*:

rVT: ou=secret, ou=confidential, ou=clearance

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

The capability to perform hierarchical evaluation on every: object, environmental and complex reference is essential for determining resource access and a significant aspect of the EDAC framework. ACL and groups are non-existent or limited in this capability.

### ***Condition Deprecator Service (CDS)***

Reference changes in a CMD due to a re-organization, salary re-structure, etc., could affect resource access because a mismatch may occur between a newly created object profile and a previously established resource condition in a resource profile. For example, say a RM establishes a reference condition from an organization structure contained in a CMD. Assume the selected reference condition requires *sales* permission to access a particular resource:

ou=sales, ou=operations, ou=ACME

Then a re-organization occurs and the *sales* department is placed under *marketing* in the CMD:

ou=sales, ou=marketing, ou=ACME

A user from the sales department will be processed with the latest reference input:

ou=sales, ou=marketing, ou=ACME

Because the reference condition was stored with the old structure (under *operations*) access will be denied. This automated constraint offers security and ensures RMs reconsider access control policies due to corporate changes. Content changes in the CMD triggers an event listener in the CDS to scan reference conditions in the repository service. Any mismatches are flagged as deprecated reference conditions in the CMS. The RM can easily identify the affected conditions and decide to edit or remove the deprecated reference condition(s).

### ***Enterprise Interoperability***

The EDAC model allows for easy expansion and interoperability among different regions. In an enterprise scenario, RMs are capable of establishing reference conditions for local and remote objects. For local objects the RM selects reference conditions from local CMDs and for remote objects the RM selects reference conditions from remote CMDs.

Figure 15 illustrates the concept.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."



Figure 15

In the illustration above a Pearl Harbor RM has established two resource profiles:

- Resource profile CPF
- Resource profile SD

The CPF resource profile allows conditional resource access only for Pearl Harbor objects and the SD resource profile allows conditional resource access only for San Diego objects. Both CPF and SD resource profiles were created by the selection of reference conditions from various CMDs applicable to local and remote objects.

"The United States Government has certain intellectual property rights in the Enterprise Dynamic Access Control software. This intellectual property is available for licensing for commercial purposes. Licensing and technical inquiries should be directed to the Office of Patent Counsel, Space and Naval Warfare Systems Center, San Diego, Code 20012, San Diego, CA, 92152; telephone (619) 553-3001, facsimile (619) 553-3821. Reference Navy Case Numbers 96217, 97188, 97189."

## Summary

To keep up with complex and growing access control requirements a scalable, enterprise and modular access control solution is required. In addition, conditional access must be capable of inheritance evaluation. The EDAC offers a concept to accomplish these vital customer requirements. Figure 16 shows a comparison among the different types of access control systems:

	Simultaneous evaluation of multiple object characteristics & environments	Simultaneous evaluation of multiple object characteristic & environmental hierarchies	Real-time detection of object characteristic changes, thus affecting resource access
ACLs	0	No	No
Groups	1	No	No
EDAC	Unlimited	Yes	Yes

Figure 16

The amount of customer participation in establishing a detailed and accurate CMD correlates to a usefulness access control service.